

---

## CHAPTER: Compliance Laws and Regulations

### SECTION: Bank Secrecy Act

### Section 400

---

#### Introduction

The Financial Recordkeeping and Currency and Foreign Transactions Reporting Act (Bank Secrecy Act or BSA), passed by Congress in 1970, requires that financial institutions file certain currency and monetary instrument reports and maintain certain records for possible use in criminal, tax, and regulatory proceedings. Failure to comply with the BSA can result in criminal or civil penalties.

The purpose of the BSA is to prevent financial institutions from being used as intermediaries for the transfer or deposit of money derived from criminal activity. Consequently, the BSA provides a paper trail of the activities of money launderers serving the interests of drug traffickers and other elements of white collar and organized crime. These activities generate large amounts of currency, often in small bills. During the course of these activities, the cash may be exchanged for larger denominations or converted to other monetary instruments for ease of use. The BSA has been amended through the years to strengthen its anti-money laundering purposes.

The Money Laundering Control Act of 1986, part of the Anti-Drug Abuse Act of 1986, strengthened the BSA by making money laundering a Federal offense. Specifically, it is a Federal crime under that Act to engage knowingly in any “financial transaction” involving proceeds derived from specified crimes if the purpose of the transaction is to: (1) promote the specified unlawful activity; (2) conceal or disguise the source, ownership, location or nature of the proceeds; or (3) evade a State or Federal transaction reporting requirement (structuring). These “financial transactions” include the movement of funds, use of one or more monetary instruments, or the use of a financial institution engaged in interstate commerce. The Act also criminalized any actual or attempted “monetary transaction” involving criminally derived property when: (1) over \$10,000 is involved; (2) a financial institution is used; (3) the property is derived from a specified crime; and (4) the transaction is conducted with the knowledge that the proceeds are criminally derived. “Monetary transaction” includes a deposit, withdrawal, transfer or exchange of funds or monetary instruments by, through or to a financial institution.

The Annunzio-Wylie Anti-Money Laundering Act, part of The Housing and Community Development Act of 1992, extended the prohibition against structuring transactions to cover international monetary instruments and increased the penalties for institutions and their employees who violate the BSA. For example, the Federal banking agencies were given the authority to revoke an institution’s charter if it is convicted of money laundering and to issue removal and prohibition orders against individuals charged with BSA offenses, unless the offense was inadvertent. The Act also increased the ceiling for assessing civil money penalties for negligent violations of the BSA to \$50,000. State-chartered institutions convicted of money laundering and BSA violations can have their deposit insurance terminated. To encourage the flow of information to the Treasury Department, the Act provided financial institutions with a “safe harbor” from civil liability under federal or state law for reporting any possible violation of law or regulation by customers. The Act also authorized the Treasury Department to issue regulations on wire transfer recordkeeping. In response, the Treasury Department and Federal Reserve Board issued a final rule, effective May 28, 1996, that requires enhanced recordkeeping related to certain funds transfers and transmittals of funds by financial institutions.

The Money Laundering Suppression Act of 1994, part of the Riegle Community Development and Regulatory Improvement Act of 1994, required the Federal banking agencies to develop enhanced examination procedures and to increase training to improve the identification of money laundering schemes in financial institutions. The Act also reduced regulatory burden by simplifying the process through which certain transactions can be exempt from reporting requirements, by reducing currency transaction reporting and by enacting other provisions to streamline the implementation of the BSA.

The BSA delegated to the Secretary of the Treasury authority for issuing regulations. Those regulations are found at 31 CFR Part 103 (Part 103). The Federal banking agencies are responsible for determining compliance by financial institutions with the BSA and implementing regulations.

Pursuant to the 1994 Act, the Federal banking agencies adopted a core set of examination procedures to determine whether an institution has the necessary system of internal controls, policies, procedures, and auditing standards to assure compliance with the BSA and implementing regulations. The procedures also require the examiner to review an institution's internal audit function, procedures, selected workpapers, records, reports, and responses. Based on the results, the examiner may conclude the review or continue with expanded procedures, which may include reviewing a sample of transactions and related documentation.

By ensuring that the institution has established policies, procedures, and practices to detect and report large cash transactions, the examiner can help deter the institution's use for money laundering. Further, the paper trail left by the institution's compliance with the recordkeeping and reporting requirements can aid in investigations of criminal activities.

### **Internal Compliance Program**

#### Office of Thrift Supervision Requirements

Office of Thrift Supervision regulations (12 CFR 563.177) require associations to establish and maintain a program to assure and monitor compliance with the requirements of the BSA and implementing Treasury regulations. The details of these requirements, such as reporting and recordkeeping, are discussed in following subsections. In brief, the program developed by an association must:

- Provide for the continued administration of the association's policies and procedures;
- Be reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements of 31 C.F.R. Part 103;
- Be reduced to writing; and
- Be approved by the board of directors and reflected in the minutes of the association.

The BSA compliance program should, at a minimum, provide for:

- A system of internal controls;

- Independent testing of compliance;
- An individual(s) to coordinate and monitor the program; and
- Training of appropriate personnel.

Operating programs and procedures established for the reporting requirements should set forth the regulatory requirements and establish compliance guidelines with respect to large cash transactions and exemptions granted to customers.

The institution should establish a record retention schedule that includes the regulatory requirements for:

- Record retention;
- Maintaining lists of exempt retail customers;
- Maintaining records for cash sales of monetary instruments between \$3,000 and \$10,000 (inclusive); and
- Customers from whom taxpayer identification numbers have not been obtained.

#### Internal Audit Function

The institution's internal audit procedures should cover:

- Reporting. Coverage of the reporting requirements should include a review of actual tellers' work and copies of filed Forms 4789 and 4790.
- Recordkeeping. Coverage of the institution's recordkeeping activities should include testing adherence to the in-house record retention schedule. This schedule should meet the requirements of the regulations.
- Exemptions. Coverage should include audit steps necessary to ascertain whether the institution is maintaining the required list of customers exempt from filing reports. The audit procedure should test the reasonableness of the exemptions granted, and verify that the list is periodically updated.
- Foreign Accounts. Coverage should require the auditor to ascertain whether the institution has

filed Form TD F 90-22.1, declaring interest in a foreign financial account, if such an account exists.

- Staff training, including attendance.
- Correction of previously deficiencies noted in audit, examination or other reports or reviews.

#### Employee Education and Training

Tellers, new accounts personnel and others handling cash should be apprised of the reporting requirements for large cash transactions.

Operations personnel should be apprised of current regulatory requirements.

The institution's management, internal auditors, tellers, new accounts staff, branch managers and personnel in cash vault operations, should be interviewed to ascertain whether they are sufficiently knowledgeable concerning the reporting and record-keeping requirements and internal operating procedures. This phase of the examination should be conducted at those offices that conduct relatively large volumes of cash business.

Personnel who have contact with customers or handle currency transactions in other departments, such as the trust, loan, international or private banking department, or the institution's subsidiaries, should also be knowledgeable of the regulations and operating procedures.

An effective education and training program is one where management periodically reinforces the importance of compliance, one that is ongoing, and one that incorporates current developments. An ongoing and updated program enables management and staff to keep abreast of regulatory changes or new money laundering schemes. The program should cover new and existing staff.

#### **Money Laundering**

Simply stated, money laundering is the intentional movement of cash through various financial institutions and/or businesses in an attempt to disguise the true source or ownership of the funds, disguise the ultimate disposition of the funds, and eliminate audit trails needed for criminal tax and fraud investi-

gations. The "legal" definition is contained in 18 U.S.C. §§ 1956 and 1957: a transaction which in any way or degree affects interstate or foreign commerce involving the movement of funds by wire or other means, or involving one or more monetary instruments, or involving the transfer of title to any real property, vehicle, vessel, or aircraft, or a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree.

Money laundering generally involves three independent steps, although these steps often occur simultaneously. First, placement, which is the process of placing, through deposits, wire transfers, or other means, unlawful cash proceeds into traditional financial institutions. Second, layering, which is the process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions. These transactions include converting cash into traveler's checks, money orders, letters of credit, stocks, and bonds, or purchasing valuable assets such as art or jewelry. Third, integration, which is the process of using an apparently legitimate transaction to disguise the illicit proceeds allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, are used.

Certain types of businesses, transactions, or geographic locations may lend themselves more readily to potential criminal activity than others. Nonetheless, attempts to launder money through a legitimate financial institution can come from many varied sources. Following are examples of potential sources of money laundering in businesses, banking functions and geographies.

*Businesses:*

- Nontraditional financial entities, including currency exchange houses, money transmitters and check cashing facilities
- Casinos
- Off-shore corporations and financial institutions located in tax or secrecy havens
- Leather-goods stores
- Car, boat, and plane dealerships
- Used automobile or truck dealers and machine parts manufacturers
- Travel agencies
- Brokers and dealers
- Jewel, gem, and precious metal dealers
- Import/export companies
- Cash-intensive businesses (e.g., restaurants, retail stores, parking garages)
- Telemarketers

*Banking functions and transactions:*

- Private banking
- Off-shore international activity
- Deposit-taking facilities
- Wire transfers or cash management functions
- Transactions in which the primary beneficiary or counterparty is undisclosed
- Loan guarantee schemes
- Traveler's checks
- Official bank checks
- Money orders
- Other electronic products that permit the rapid movement of currency (e.g., foreign exchange transactions followed by payment into another jurisdiction)

- Trade financing transactions with unusual pricing features

*High risk geographies:*

- Countries in which the production of illegal drugs may be taking place
- Areas in which money launderers may seek to deposit funds due to the absence of bank secrecy laws
- Emerging countries which may be seeking hard currency investments
- Major money laundering countries identified in the U.S. Department of State's *International Narcotics Strategy Annual Report*.

A savings association should have policies and procedures designed to detect and prevent money laundering activities as part of its written BSA compliance program. An effective program should:

- Define the different forms of money laundering;
- Provide compliance with BSA and related anti-money laundering laws and regulations;
- Establish a "Know Your Customer" program; and
- Identify high risk activities, businesses and foreign countries commonly associated with money laundering.

An effective anti-money laundering program should extend to all of the association's operations, including retail, fiduciary, loan, private banking, etc. (refer to the Examination Procedures for a more complete list).

An effective anti-money laundering program should have as its cornerstone a high level of internal controls to minimize the risk of money laundering. Those controls should include, at a minimum: (1) money laundering detection procedures; (2) identification and monitoring of non-bank financial institutions that are depositors of the institution and that engage in a high volume of cash activity; (3) periodic account activity monitoring; and, (4) internal investigations, monitoring and reporting of suspicious transactions.

Money laundering activities are discussed in further detail in the “Know Your Customer” and “Suspicious Activities” subsections. Other subsections, such as “Education and Training” also include money laundering elements.

### “Know Your Customer”

Note: Although the proposed “Know Your Customer” (KYC) regulation was withdrawn, savings associations need to guard against money laundering and identify suspicious activities. An effective anti-money laundering program is expected in all savings associations. Examiners will review the program adopted by the savings association, determine its ability to adequately identify and control the risks of exposure to money laundering activities, and evaluate the savings association’s adherence to the program

Illicit activities, such as money laundering, fraud and other transactions designed to assist criminals in their illegal ventures, pose a serious threat to the integrity of financial institutions. The exposure of these activities damages the reputation of the institution and may subject it to criminal proceedings. An effective KYC policy, coupled with effective procedures for reporting suspicious transactions, can help protect the institution against money laundering activity and other financial crimes by minimizing the risk that the institution will be used for illicit activities. An effective policy also helps protect the institution’s reputation, detect suspicious activity in a timely manner, and reduces the risk of government seizure and forfeiture of a customer’s loan collateral. For these reasons, savings associations are strongly encouraged to adopt KYC policies.

### Objectives

An effective KYC policy should contain a clear statement of management’s overall expectations and establish specific line responsibilities. The objectives of a KYC policy are to:

- Facilitate the institution’s compliance with applicable laws and regulations, including the BSA and OTS’s compliance (12 CFR 563.177) and suspicious activity reporting regulations (12 CFR 563.180);

- Facilitate safe and sound banking practices;
- Decrease the likelihood that the institution will become a victim of illegal activities perpetrated by its “customers;”
- Protect the good name and reputation of the institution; and
- Not interfere with the relationship of the institution and its legitimate customers.

### Contents

An association’s KYC policy should be appropriate to its size, location, and complexity of business. It should also reflect the types of customers it serves, the nature and extent of their activities at the association, and other factors that the association considers in its assessment of the risks associated with its customers and their transactions. An effective KYC policy should enable the association to understand the kinds of transactions that particular customers are likely to engage in. Therefore, the association should collect sufficient information to develop a customer profile to ensure compliance with the suspicious activity reporting requirements.

An effective KYC policy should incorporate the following principles into the association’s business practices:

- Determine the true identity of all customers requesting its services;
- Determine the customer’s source(s) of funds for transactions involving the association;
- Determine the particular customer’s normal and expected transactions involving the association;
- Monitor customer transactions to determine if they are consistent with the normal and expected transactions for that customer or for similar categories or classes of customers established by the association;
- Identify customer transactions that do not appear to be consistent with normal and expected transactions for that particular customer or for customers in similar categories or classes; and

- Determine if a transaction is unusual or suspicious in accordance with 12 CFR 563.180 and, if so, report those transactions.

Further, an effective KYC policy should provide for and document the following features to ensure compliance with the association's KYC program:

- A system of internal controls to ensure ongoing compliance;
- Independent testing for compliance;
- An individual(s) responsible for coordinating and monitoring day-to-day compliance; and
- Training to all appropriate personnel on a regular basis regarding the content and procedures of the KYC policy or program.

#### Identifying the Customer

A relationship with an association should generally not be established until the identity of a potential customer is satisfactorily established. The following general principles can be followed when establishing customer relationships:

##### *Personal Accounts*

- Require satisfactory identification to open an account (e.g., a driver's license with a photograph issued by the state in which the association is located; or a U.S. passport or alien registration card together with a college photo identification card, a major credit card (verify the current status), an employer identification card, and/or a current utility bill from the customer's present address).
- Consider the location of the customer's residence or place of business. If it is not in the area served by the association's office or branch, question why the customer is not opening an account at that location.
- Call the customer's residence or place of employment to thank him or her for opening the account. Disconnected phone service or no record of employment warrant further investigation.

- Consider the source of funds used to open the account. Large cash deposits should be questioned.
- For large accounts, ask the customer for a prior financial institution reference and, if appropriate, write a letter to the institution asking about the customer.
- Check with service bureaus for indications the customer has been involved in questionable activities such as kiting incidents and NSF situations.
- The identity of a customer may be established through an existing relationship with the institution such as some type of loan or other account relationship.
- A customer may be a referral from an association employee or one of the association's accepted customers. A referral alone is not sufficient to identify the customer, but in most instances should warrant less vigilance than otherwise required.

##### *Business Accounts*

- Ask business principals for evidence of legal status to open a business account (e.g., sole proprietorship, partnership, or incorporation or association).
- Determine the beneficial ownership of accounts in private banking, fiduciary departments, and other specialized departments. The association should pay particular attention to corporate entities, international business corporations, bearer share companies, or nominee officers, especially if those organizations are based in jurisdictions with minimal money laundering laws.
- For payable through accounts with foreign banks, require satisfactory identification for all sub-account holders.
- Check the name of a commercial enterprise with a reporting agency and check prior bank references.

- Call the customer's business to thank him or her for opening the account. Disconnected phone service warrants further investigation.
- If appropriate, visit the business to verify its existence and its ability to provide the services described.
- Consider the source of funds used to open the account. Large cash deposits should be questioned.
- Especially for large commercial accounts, obtain a:
  - Financial statement of the business;
  - Description of the customer's principal line of business;
  - Description of the business's primary trade area, and whether international transactions are expected to be routine; and
  - Description of the business operations, such as retail versus wholesale, and the anticipated volume of cash sales.

An effective BSA compliance program also recognizes that certain customer transactions are suspicious in nature. A savings association must know its customers to be able to make an informed decision as to the suspicious nature of a particular transaction. The following subsection discusses potentially suspicious activities that may warrant further review or investigation.

### Suspicious Activities

#### Suspicious Conduct and Transactions

There are certain categories of conduct or activities that are suspicious in nature and should alert a savings association to the potential for the customer to conduct illegal activities. Examples are grouped by topic and provided below.

*Activities that may be inconsistent with the customer's business:*

- A customer opens several accounts for the type of business he or she purportedly is conducting or frequently transfers funds among these accounts.
- A customer's corporate account(s) has deposits or withdrawals primarily in cash rather than checks.
- The owner of both a retail business and a check cashing service does not ask for cash when depositing checks, possibly indicating the availability of another source of cash.
- The customer's account has unusual activity in cash purchases of money orders and cashier's checks.
- A large volume of cashier's checks, money orders, or wire transfers are deposited into an account in which the nature of the account holder's business would not appear to justify such activity.
- A customer frequently makes large bill transactions (such as deposits, withdrawals, or purchases of monetary instruments) without an explanation as to how it will be used in the business or the purchases allegedly are for a business that generally does not deal in large amounts of cash.
- Business account history that shows little or no regular, periodic activity; the account appears to be used primarily as a temporary repository for funds that ultimately are transferred abroad.
- A customer's place of business or residence is outside the financial institution's service area.
- A corporate customer who frequently makes large cash deposits and maintains high balances, but does not use other banking services.
- The customer routinely makes numerous deposits of checks from a retail business but rarely makes cash withdrawals for daily operations.
- A retail business has dramatically different patterns of cash deposits from similar businesses in the same general location.
- The currency transaction patterns of a business experience a sudden and inconsistent change from its normal business activities.

- The amount and frequency of cash deposits are inconsistent with the activity observed at the customer's place of business.
- The business frequently deposits large amounts of cash, but checks or other debits drawn against the account are inconsistent with the customer's retail business.
- Businesses that do not normally generate currency make numerous currency transactions.
- Financial transactions involving monetary instruments that are incomplete or contain fictitious payees, remitter, etc., if known.
- Unusual transfer of funds among related accounts or accounts that involve the same principal or related principals.
- A business owner, such as an owner who has only one store, who makes several deposits the same day using different branches.
- Frequent deposits of currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Frequent deposits of musty or extremely dirty bills.
- A customer who purchases cashier's checks, money orders, etc., with large amounts of cash.
- A professional customer who makes substantial deposits of cash into client accounts or in-house company accounts, such as trust and escrow accounts.
- Domestic accounts opened in the name of a *casa de cambio* (money exchange house), followed by suspicious wire transfers or structured deposits into these accounts.
- Suspicious movements of funds out of one institution into a second one and back into the first institution. For example, the following scheme has been observed: (1) purchasing cashier's checks from bank A; (2) opening a checking account at bank B; (3) depositing the cashier's checks into bank B's checking account; and (4) wire transferring the funds out of the checking account at bank B to an account at bank A.

*Other suspicious customer activities:*

- A substantial deposit of numerous \$50 and \$100 bills.
- A mailing address outside the United States.
- Frequent exchanges of small and large bills.
- A certificate(s) of deposit or other investment vehicle used as collateral for a loan.
- A large problem loan is suddenly paid down with no reasonable explanation of the source of funds.
- Excessive use of safe deposit boxes or changing traffic patterns in the safe deposit box areas.
- A safety deposit box is often accessed before the customer makes cash deposits which are just under the threshold for reporting the transaction.
- A customer who rents multiple safe deposit boxes.
- Frequent deposits of large amounts of currency wrapped in currency straps that have been stamped by other financial institutions.
- Offshore companies, especially those located in bank secrecy haven countries, ask for a loan from a domestic U.S. bank or for a loan secured by obligations of offshore banks.
- Use of loan proceeds in a manner inconsistent with the stated purpose of the loan.
- A nonaccount holder who purchases a monetary instrument with large denominated bills.
- A customer who purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold, or without apparent reason.
- Couriers, rather than personal account customers, make the deposits to the account.
- Money orders, deposited by mail that have unusual symbols or stamps on them.

*Conduct and activities that may indicate avoidance or reporting or recordkeeping requirements:*

- A business or new customer asks to be placed on the association's exemption list.
- Frequent requests for increases in exemption limits.
- An urgent request to be included on the association's exemption list.
- A customer who tries to engage in a transaction in excess of a specified threshold who, when advised of the recordkeeping or reporting requirements, withholds part of the currency deposit to keep the transaction under that threshold.
- A customer who is reluctant to provide the information needed to file the mandatory report, or have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer or group tries to coerce an association employee into not filing any required recordkeeping or reporting forms.
- An automatic teller machine is used to make several deposits below a specified threshold.
- Unusually large deposits of U.S. food stamps (often used as currency in exchange for narcotics).
- A customer who is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

*Activities related to fund (wire) transfers:*

- Sending and receiving wire transfers to or from bank secrecy haven countries without an apparent business reason or when they are inconsistent with the customer's business or history.
- Periodic wire transfers from a personal account(s) to bank secrecy haven countries.
- Frequent or a large volume of wire transfers to and from offshore institutions (banking centers).

- Deposits of funds into several accounts, usually in amounts below a specified threshold, which are subsequently consolidated into one master account and transferred outside of the country.
- A customer makes large volumes of deposits to several different accounts and subsequently frequently transfers major portions of the balances to a single account at the same or another financial institution.
- Instructions to a financial institution to wire transfer funds abroad and to expect an incoming wire transfer of funds, in an equal amount, from other sources.
- Regular deposits or withdrawals of large amounts of cash, using wire transfers to, from, or through countries that are either known sources of narcotics or whose laws are ineffective in controlling the laundering of money.
- • Wire transfers received and monetary instruments purchased immediately for payment to another party.

*Conduct that may indicate insufficient or suspicious information by a customer:*

- The reluctance of a business which is establishing a new account to provide complete information about the purpose of business, its prior banking relationships, names of its officers and directors, and information about the location of the business.
- A customer's refusal to provide the usual information necessary to qualify customers for credit or other banking services.
- A customer's unwillingness to provide personal background information when opening an account or purchasing monetary instruments above a specified threshold.
- A customer who desires to open an account without providing references, a local address, or identification, or who refuses to provide any other information the association requires to open an account.
- Unusual or suspicious identification documents that the association cannot readily verify.

- The discovery that a customer's home phone is disconnected.
- No record of past or present employment on a loan application.
- A customer who makes frequent or large transactions who has no record of past or present employment experience.
- The customer's background varies with his or her business activities.
- The customer is reluctant to reveal details about business activities or to provide business financial statements.
- The customer's financial statements differ from those of similar businesses.

*Employee activities:*

- Lavish lifestyle cannot be supported by an employee's salary.
- Reluctance to take a vacation.

*Institution to institution transactions:*

Significant changes in currency shipment patterns between correspondent institutions.

Larger amounts of cash without a corresponding increase in the filing of mandatory CTRs.

Deposits with the Federal Reserve Bank or its branches are disproportionate to the previous historical volume(s) of similarly sized financial institutions.

Significant turnover in large denomination bills that would appear uncharacteristic given the association's location.

CTRs, when filed, are frequently incorrect or incomplete.

A large increase in small denomination bills and a corresponding decrease in large denomination bills with no corresponding CTR filings.

The rapid increase in the size and frequency of cash deposits with no corresponding increase in noncash deposits.

Reporting

Note: OTS regulations (12 CFR 563.180) are not limited to money laundering and BSA violations. They apply to any possible violation of federal law or regulation that meet the regulatory criteria. These other activities, such as robberies, are more fully discussed in Section 405, Bank Protection Act.

Effective April 1, 1996, savings associations and their service corporations are required by section 563.180 to file a suspicious activity report (SAR) when they detect a known or suspected violation of Federal law or a suspicious transaction related to a money laundering activity or a violation of the BSA.

A SAR is required to be filed for any known or suspected Federal criminal violation, or pattern of criminal violations: (1) involving insider abuse in any amount, (2) aggregating \$5,000 or more where a suspect can be identified; or (3) aggregating \$25,000 or more regardless of a potential suspect.

A SAR is also required to be filed for any transaction conducted or attempted by, at or through the savings association or service corporation and aggregating \$5,000 or more, if the savings association or service corporation knows, suspects, or has reason to suspect that the transaction:

- May involve potential money laundering (referred to in the regulations as illegal activities);
- Is designed to evade the BSA or its implementing regulations; or
- Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts.

"Transaction" is broadly defined using the definition of money laundering found in 18 U.S.C. §§ 1956 and 1957. Consequently, transaction includes a deposit, withdrawal, transfer between accounts,

exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by what ever means effected.

A savings association is required to file a SAR with FinCEN (OTS has access to the SAR through FinCEN) no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, a savings association may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case can the reporting be delayed more than 60 calendar days.

In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, a savings association is required to immediately notify, by telephone, an “appropriate law enforcement authority” and the OTS in addition to filing a timely SAR. An “appropriate law enforcement authority” generally would be the local office of the IRS, Criminal Investigation Division or the FBI.

### **Reporting Requirements**

The reports that financial institutions are required to file are:

- Reports of Suspicious Transactions (31 CFR 103.21);
- Reports of Currency Transactions (31 CFR 103.22);
- Reports of Transportation of Currency or Monetary Instruments (31 CFR 103.23);
- Reports of Foreign Financial Accounts (31 CFR 103.24);
- Reports of Transactions With Foreign Financial Agencies (31 CFR 103.25); and
- Reports of Certain Domestic Coin and Currency Transactions (31 CFR 103.26).

This Handbook covers the first four reports. The first three reports are included as Exhibits A, B and C.

#### Suspicious Activity Report (OTS Form 1601)

A Suspicious Activity Report (SAR) must be filed for any transaction involving \$5,000 or more when the institution knows, suspects, or has reason to suspect that a transaction:

- Involves money laundering;
- Is designed to evade BSA regulations; or
- Has no business or apparent lawful purpose or is not the type that the customer would normally be expected to undertake.

The SAR must be filed with the U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN) within 30 days after the initial detection of facts giving rise to an SAR filing. If no suspect was initially identified, the SAR may be delayed for an additional 30 calendar days to identify a suspect. The “Suspicious Transactions” subsection contains a more detailed discussion of the SAR and suspicious activities.

#### Currency Transaction Report (Form 4789)

A Currency Transaction Report (CTR) must be filed for each transaction in currency (deposit, withdrawal, exchange or other payment or transfer) of more than \$10,000. A completed CTR must be filed with the Internal Revenue Service (IRS) within 15 days after the date of the transaction. Multiple transactions totaling more than \$10,000 during any one business day are treated as a single transaction if the institution has knowledge that they are by or on behalf of any person. Certain types of currency transactions need not be reported, such as those involving “exempt persons” or those generated by particular retail or commercial customers meeting specific criteria for exemption. These exemptions are discussed below.

#### Currency and Monetary Instrument Report (Form 4790)

A Currency and Monetary Instrument Report (CMIR) must be filed for each shipment of currency

or other monetary instrument(s) in excess of \$10,000 out of or into the U.S., except via the postal service or common carrier. When a person physically transports monetary instruments into or out of the U.S., a CMIR must be filed with the appropriate U.S. Customs officer or the Commissioner of Customs at the time of entry into or departure from the U.S. When a person receives monetary instruments shipped from any place outside the U.S., a CMIR must be filed with the appropriate U.S. Customs officer or the Commissioner of Customs within 15 days of receipt of the receipt of the instruments (unless a report has already been filed).

#### Report of Foreign Financial Accounts (Treasury Form 90-22)

Each person subject to U.S. jurisdiction with a financial interest in, or signature authority over, a bank, securities, or other financial account in a foreign country must file a Report of Foreign Bank Financial Accounts concerning such relationship with the IRS annually.

#### Amended Reports

Institutions should file an amended report if they have failed to make appropriate corrections as a result of correspondence from the IRS or a form fails to provide critical information. The IRS expects forms to be typed or printed legibly. When the IRS requires a response, the institution should make that response within 10 days.

#### **Exemptions From Reporting Large Currency Transactions**

(Note: On September 7, 1997, Treasury published a notice of proposed rulemaking that would further modify the rules for granting exemptions from the currency transaction report filing requirements. That proposal is not included in this Handbook section.)

#### Background

Treasury regulations have historically recognized that routine reporting of some large currency transactions does not necessarily aid law enforcement authorities and, at the same time, may place unreasonable burdens on financial institutions. Consequently, a financial institution may be exempt from filing CTRs on certain types of customers who regularly deal in large amounts of currency. For example, a financial institution may be exempt if the amount of currency involved with a customer does not exceed what that customer typically receives from a lawful business.

The Money Laundering Suppression Act of 1994 (MLSA) requires a two-tier exemption system. Under the first tier, or “mandatory” exemptions, cash transactions of governments, financial institutions and major businesses are not reportable. The second tier, or “discretionary” exemptions, addresses smaller businesses. A third category of exemptions contained in Part 103 addresses certain designated organizations.

#### Mandatory Exemptions (31 CFR 103.22(h))

Under the MLSA, as implemented by FinCEN’s final rule dated September 7, 1997 and effective January 1, 1998, a financial institution is not required to file a CTR for transactions by “exempt persons.” The final rule permits – but does not require – financial institutions to use the simplified exemption procedures for certain types of customers. A financial institution may choose to operate under the previous, more labor-intensive procedures (discussed in the following section). However, the institution will remain subject to all of the regulatory requirements and penalty rules. In contrast, the revised exemption procedures afford financial institutions a limitation on liability.

The previous rules required a separate exemption for each account, regardless of the institution’s ability to monitor daily aggregate transactions. The final rule exempts customers, not accounts. It places no limit on the dollar amount of an exemption. The final rule also extends the exemption to all transactions; the prior rule is limited to deposits and withdrawals.

The final rule identifies six categories of “exempt persons”:

1. A bank, to the extent of its domestic operations;
2. A federal, state or local government agency or department;
3. Any entity exercising governmental authority within the U.S.;
4. Any entity (other than a bank) whose common stock is listed on the New York, American, or NASDAQ stock exchanges (with some exceptions);
5. Any subsidiary (other than a bank) of any “listed entity” that is organized under U.S. law and at least 51 per cent of whose common stock is owned by the listed entity; and
6. Any non-bank financial institution that is, or is a subsidiary of, a listed entity, to the extent of its domestic operations.

To assure itself that a customer is exempt, an institution must take steps comparable to those that a reasonable and prudent institution would take and document to protect itself from loan or other fraud or loss based on misidentification of a person’s status. The final rule includes “operating rules” (31 CFR 103.22(h)(4)) detailing these steps. To summarize:

- For banks and government agencies, the same documentation an institution receives authorizing the establishment of a business account is generally sufficient (e.g., a corporate resolution). Any documentation that demonstrates that a customer is a bank is sufficient. In the case of small governmental units, such as a volunteer fire department, an institution may rely on reasonable documentation, based on the type and nature of the governmental agency involved.
- For entities exercising governmental authority, such as the New Jersey Turnpike Authority or the Port Authority of New York, an institution must determine and document the characteristics that make such an authority governmental in nature, such as the authority to exercise emi-

nent domain, the authority to tax the public, or the authority to routinely exercise police powers.

- For listed corporations, an institution may consult newspapers or weeklies to determine if a company is listed on an exchange. An institution may also rely on information available electronically from the SEC or on stock exchange Web sites.
- For subsidiaries, any reasonable documentation will be sufficient, including a letter signed by a company officer, a tax return or the entity’s Annual Report of Form 10-K.
- Franchises are not exempt simply because the company that awards the franchise license is exempt. The institution must determine whether the franchise is itself a publicly traded corporation or its consolidated subsidiary.

To take advantage of this exemption procedure, an institution must designate a customer as an exempt person within 30 days of a reportable transaction and stop filing CTRs. A designation of exemption is made by filing a single CTR in which Part I, Section A and Part III are fully completed and box 36 is marked “Designation of exempt person.”

Financial institutions will not be penalized for using reasonable judgment with regard to designating exemptions under the final rule, even if that judgment is occasionally wrong. However, an institution remains subject to a penalty if it knowingly files false or incomplete information or has reason to believe at the time of exemption that the customer is not eligible or that the transaction is not a transaction of the exempt person.

Finally, an institution is required to verify the status of those entities it has designated as exempt persons once a year, unless there is reason to believe that a customer no longer meets the exemption criteria or someone other than the exempt person engages in the transaction.

Exemptions Involving Designated Organizations  
(31 CFR 103.22(b))

CTRs need not be filed:

- For transactions with Federal Reserve or Federal Home Loan Banks;
- For transactions between domestic banks; or
- By nonbank financial institutions for transactions with commercial banks (however, commercial banks must report transactions with nonbank financial institutions).

Discretionary Exemptions (31 CFR 103.22(c))

Financial institutions may exempt certain transactions of certain retail or commercial customers in amounts commensurate with the customary and lawful business operations of that customer. These exemptions must be in accounts which the financial institution may reasonably conclude do not exceed amounts commensurate with the customary conduct of the lawful, domestic business of that customer. These exemptions include:

- Deposits or withdrawals of currency from an existing account by an established depositor who is a U.S. resident and operates a domestic retail business;
- Deposits or withdrawals of currency from an existing account by an established depositor who is a U.S. resident and operates a sports arena, race track, amusement park, bar, restaurant, hotel, licensed check cashing service, vending machine company, theater, regularly scheduled passenger carrier or any public utility;
- Deposits or withdrawals, exchanges of currency or other payments and transfers by federal, state or local governments or agencies; or
- Withdrawals for payroll purposes from an existing account by an established depositor who is a U.S. resident and operates a firm that regularly withdraws more than \$10,000 to pay its employees.

Exemption Lists; Recordkeeping Requirements (31 CFR 103.22(d) and (f))

An institution may only place those customers on its exempt list who attest to the basis for the exemption in a written statement that describes the customary conduct of the business and a detailed statement of reasons why that customer is qualified for an exemption. The statement shall include the name, address, nature of business, taxpayer identification number and account number of the customer being exempted. The regulation also requires a certification statement, the form and content of which is specifically described in section 103.22(d).

An institution is responsible for independently verifying the account activity and determining dollar limits for exempted deposits or withdrawals. The exempted transactions must be in amounts that the institution may reasonably conclude do not exceed amounts commensurate with the customary conduct of the lawful domestic business of that customer.

An institution must keep a record of each exemption granted and the reason for granting the exemption in a centralized list. The record must include: (1) the names and addresses of domestic banks or correspondent banks with whom the financial institution conducts transactions; and, (2) the name, address, business, taxpayer identification number and account number of each depositor that has engaged in currency transactions that have not been reported due to the granting of a “discretionary” exemption. The later record must also indicate whether the exemption covers withdrawals, deposits, or both, and the dollar limit of the exemption.

Lists that appear inordinately long or that contain names of customers whose business size or nature would not ordinarily merit exempt status should be discussed with management. If management cannot provide adequate explanation or supporting documentation, the matter should be reported.

Management is also responsible for reviewing and updating the exempt list to ensure the continued exempt status of customers, to add new exemptions, and to delete customers who no longer qualify for exempt status. Treasury recommends review at least annually.

**Effect on Other Regulatory Requirements**

The mandatory exemption procedures do not create any exemption, or have any effect at all, on the requirement that financial institutions file suspicious activity reports. Similarly, a customer's status as an exempt person has no impact on other BSA requirements relating to record retention or reporting. For example, the fact that a customer is an exempt person has no effect on the obligation of a financial institution to retain records of funds transfers by that person, or to retain records in connection with the sale of cashier's checks to that person.

If an institution has improperly exempted accounts, the examiner can instruct the institution's management to remove the account from the exemption list, begin filing CTRs, and write to the IRS Detroit Computing Center for a determination on whether backfiling of unreported transactions is necessary. The decision to backfile CTRs rests with FinCEN.

Financial institutions who wish to obtain more information about the currency exemption process should review the Treasury's Currency and Foreign Transactions Reporting Act Exemption Handbook or contact the Treasury's Financial Crimes Enforcement Network (FinCEN) at 1-800-949-2732 or 703-905-3920.

**Recordkeeping Requirements**

The following summarizes the significant BSA recordkeeping requirements. The summary is not all-inclusive: some requirements contain an additional level of detail, and others contain some exceptions.

An institution must develop and maintain a properly completed exemption list centralized in one location, with detailed supporting documentation. See the "Exemptions from Reporting Large Currency Transactions" subsection, the Examination Procedures and 31 CFR 103.22 for the detailed recordkeeping requirements.

Institutions are prohibited from issuing or selling monetary instruments (e.g., bank checks or drafts, cashier's checks, money orders or traveler's checks) in amounts between \$3,000 and \$10,000 unless the institution verifies the identity of the customer and maintains detailed supporting documentation, in-

cluding the name of the purchaser, date of purchase, type of instrument purchased, etc. See the "Cash Sales of Monetary Instruments" subsection, Examination Procedures and 31 CFR 103.29(a) for the detailed recordkeeping requirements.

An institution must collect and retain certain information in connection with wire (fund) transfers of \$3,000 or more. The information required to be collected and retained depends upon the type of financial institution, its role in the wire transfer (originator, intermediary, or beneficiary), the amount of the wire transfer, and the relationship of the parties to the transaction with the financial institution. See the Examination Procedures and 31 CFR 103.33(e) and (g) for the detailed recordkeeping requirements.

Section 103.33 also requires financial institutions to retain:

- Documentation to support each extension of credit over \$10,000 (except when the extension is secured by an interest in real property);
- Each advice, request, or instruction received regarding a transaction that results in the transfer of funds, currency, checks, investment securities, other monetary instruments or credit, of more than \$10,000 to a person, account, or place outside the United States; and
- Each advice, request, or instruction given to another financial institution or other person located within or outside the United States, regarding a transaction intended to result in a transfer of funds, currency, checks, investment securities, other monetary instruments or credit, of more than \$10,000, to a person, account, or place outside the United States.

Section 103.34 requires financial institutions to keep the following records:

- A list of each individual who holds a deposit account for which the institution has been unable to secure a taxpayer identification number;
- Each document granting signature authority over each deposit account;
- Each statement, ledger card, or other record of each deposit account;

- Each document relating to a transaction of more than \$10,000 remitted or transferred to a person, account or place outside the United States;
- Each check or draft in excess of \$10,000 drawn on or issued by a foreign bank that the domestic bank has paid or presented to a nonbank drawee for payment;
- Each item relating to any transaction over \$10,000 received on any one occasion directly and not through a domestic financial institution, from a bank, broker, or dealer in foreign exchange outside the United States;
- Records prepared or received by a bank in the ordinary course of business that would be needed to reconstruct a demand deposit account and to trace a check in excess of \$100 deposited in such demand deposit account;
- A record containing certain specified information of any person presenting a certificate of deposit for payment, and a description of the instrument and date of the transaction; and
- Each deposit slip or credit ticket reflecting a transaction in excess of \$100 or the equivalent record for direct deposit or other wire transfer deposit transactions.

Finally, each of the reports discussed in the “Reporting Requirements” subsection include record-keeping requirements.

An institution is required to retain either the original, microfilm, copy or other reproduction of the relevant documents. All records must be retained for at least 5 years. Records required to be retained by the reporting requirements may be those made in the ordinary course of business by an institution. If no record is made in the ordinary course of business in connection with any transaction where records are required to be retained, a record must be prepared in writing by the institution.

All required records – the identifying information as well as information about the transaction—must be filed or stored in such a way as to be accessible within a reasonable period of time, taking into consideration the nature of the record and the amount of time expired since the record was made. The retrievability of records in connection with wire

(fund) transfers is discussed separately in that subsection.

### **Sale of Monetary Instruments**

Financial institutions sell a variety of monetary instruments for cash (e.g., bank checks or drafts including foreign drafts, money orders, official checks and traveler’s checks). Purchasing these instruments in amounts of less than \$10,000 is a common method used by money launderers to evade large currency transaction reporting requirements. Once converted from cash, criminals typically deposit these instruments in aggregation accounts with other depository institutions to facilitate the movement of funds through the payment system. In many cases, the individuals involved do not have an account with the institution from which the instruments are purchased.

Section 103.29 of Treasury’s regulations requires institutions to verify the identity of individuals purchasing monetary instruments with currency in amounts between \$3,000 and \$10,000, inclusive, and to maintain records of all such sales.

Institutions may either verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the institution or may verify the identity of the purchaser by viewing a piece of identification that contains the customer’s name and address and is acceptable within the banking community as a means of identification when cashing checks for noncustomers. The method used to verify the identity of the purchaser must be recorded.

Treasury’s Administrative Ruling 92-1 provides guidance on how an institution can verify the identity of an elderly or disabled customer who does not possess the normally acceptable forms of identification. An institution may accept a social security card or Medicare/Medicaid card along with another form of documentation bearing the customer’s name and address. The additional documentation may be in the form of a utility bill, a tax bill, or voter registration card. The forms of alternate identification an institution decides to accept must be included in the formal policies and procedures.

Part 103 provides that the records of sales must contain, at a minimum, the following information:

If the purchaser has a deposit account with the association:

- the name of the purchaser;
- the date of purchase;
- the type(s) of instrument(s) purchased;
- the serial number(s) of each of the instrument(s) purchased;
- the dollar amount(s) of each of the instrument(s) purchased in currency; and
- the method of verification of identity, and

If the purchaser does not have a deposit account with the association:

- the name and address of the purchaser;
- the social security or alien identification number of the purchaser;
- the date of birth of the purchaser;
- the date of purchase;
- the type(s) of instrument(s) purchased;
- the serial number(s) of each of the instrument(s) purchased;
- the dollar amount(s) of each of the instrument(s) purchased; and
- the method of verifying the identity of the purchaser and specific identifying information (e.g. State of issuance and number of driver's license).

If the required information cannot be provided by the purchaser at the time of the transaction or by the association's own previously verified records, the transaction must be refused.

Contemporaneous purchases of the same or different types of instruments totaling \$3,000 or more must be treated as one purchase. Multiple purchases during one business day totaling \$3,000 or more must be aggregated and treated as one purchase if the association has knowledge that the purchases have occurred. The records of monetary instrument

sales must be retained for 5 years and be available to the Secretary of the Treasury upon request.

### **Wire Transfers**

The primary purpose of the BSA is to identify the sources, volume, and movement of funds. Historically, money laundering activity centered around currency-based transactions. However, recent evidence indicates that the funds transfer systems are not immune to illegal activity. The BSA was amended by the Annunzio-Wylie Anti-Money Laundering Act of 1992 to authorize Treasury and the Federal Reserve Board to prescribe regulations regarding domestic and international funds transfers. In January 1995 the Treasury and the Board issued a final rule, effective May 28, 1996, on recordkeeping and retrieval requirements concerning payment and transmittal orders by financial institutions. The rule requires each domestic financial institution involved in funds transfer to collect and retain certain information depending upon the type of financial institution, its role in the particular wire transfer, the amount of the wire transfer, and the relationship of the parties to the transaction with the financial institution.

The FFIEC has also adopted a policy statement on money laundering activities involving large-value funds transfers (TB 57). The policy statement encourages all financial institutions to record in the message text of the order the name, address, and account number of both the originator and beneficiary to the transaction. This includes payment orders sent through Fedwire, CHIPS, SWIFT, and any proprietary networks. OTS also encourages all savings associations to modify their existing wire transfer procedures to ensure the provisions of the policy statement are followed.

### **Payable Through Accounts**

A payable through account (PTA) is a demand deposit account through which banking entities located in the U. S. extend check-writing privileges to the customers of a foreign bank operating outside the U.S. Under this arrangement, a U. S. bank, Edge corporation or the U. S. branch or agency of a foreign bank opens a master checking account in the name of the foreign bank. The foreign bank subsequently divides the master account into sub-

accounts in the name of one of the foreign bank's customers. Deposits into the master account may flow through the foreign bank, which pools them for daily transfer to the U. S. banking entity, or the funds may flow directly to the U. S. banking entity for credit to the master account, with further credit to the sub-account.

PTA activities differ from traditional correspondent banking relationships in that correspondent relationships typically involve an arrangement under which bank "A" processes and completes transactions for bank "B's" customers or bank "B" itself. Under that arrangement, Bank B's customers are generally not aware of the correspondent relationship and do not have access to Bank B's account at Bank A. In a PTA relationship, the sub-account holders have direct control of the PTA due to their signatory authority over the foreign bank's account at the U.S. banking entity.

Although the use of PTAs by savings associations has been relatively rare, recent evidence suggests that some financial institutions may not be exercising the same degree of care regarding these accounts that they exercise for domestic customers. For example, an institution may simply collect signature cards that have been completed abroad and then process checks issued by sub-account holders. These institutions undertake little or no effort to independently obtain or verify information about the individuals and businesses who use their accounts.

The Federal banking agencies are concerned, based on recent reports from law enforcement agencies and their own investigatory efforts, that the lack of safeguards over these accounts may facilitate unsafe and unsound banking practices, including money laundering and related criminal activities. Consequently, savings associations are encouraged to become familiar with PTAs and to develop and maintain procedures, as appropriate to their activity, to guard against possible improper or illegal use of payable through accounts.

Adopted procedures should enable a savings association offering PTA services to foreign banks to identify the ultimate users of its foreign bank customers' PTAs. The institution should have the ability to review, and obtain when necessary, the same type of information on each ultimate user of its payable through service as the institution obtains

for its domestic customers. If the institution is unable to appropriately review the identifying information, steps should be taken to terminate the payable through relationship as expeditiously as possible.

### **Economic Sanctions**

The Office of Foreign Assets Control (OFAC) of the U. S. Department of the Treasury is responsible for administering a series of laws that impose economic sanctions against select foreign countries to further U.S. foreign policy and national security objectives. Compliance with OFAC regulations by financial institutions requires the blocking of accounts of certain countries or individuals under certain circumstances. Because some of those circumstances relate to money laundering, an effective know your customer program is an important component of ensuring compliance with OFAC regulations. Section 415 of the OTS Compliance Activities Handbook contains information on economic sanctions and a copy of OFAC regulations.

### **Examination Objectives**

1. To determine whether the institution's operating policies, procedures and practices are adequate to enable management or other responsible personnel to readily identify all of the currency and monetary transactions covered by the BSA.
2. To determine whether policies and procedures have been implemented covering the detection and prevention of money laundering activities or BSA violations.
3. To evaluate the effectiveness of the institution's compliance program for the BSA, including identifying suspicious transactions that may involve money laundering activity.
4. To ascertain whether established compliance guidelines and operating procedures are regularly tested by independent personnel.
5. To verify that the institution completes and maintains all applicable records required by the BSA regulations.
6. To verify that the institution files accurately and within specific time limits the required

forms for the various types of currency and monetary instrument transactions.

7. To determine the institution's compliance with the BSA and its implementing regulations.

### **Examination Procedures**

1. The purpose of the examination procedures is to determine whether the financial institution has developed written policies, operating procedures, and reliable methods to record and report the data necessary for compliance with the Bank Secrecy Act and implementing Treasury and OTS regulations and to detect and/or prevent money laundering activities. The procedures are designed to maximize the efficiency of the review process by using sampling or by requiring the institution to perform some analyses. Consistent with the examination approach discussed in Section 105 of this Handbook, the specific procedures performed during an examination may vary depending on whether the examiner discovers problems or internal control weaknesses. Some procedures require sampling, which may be completed by the examiner or by the institution.
2. The narrative to this Handbook section contains detailed information on how to report and detect suspicious activities. The examination procedures do not contain a specific subsection on suspicious activities because they can be identified by performing procedures in various areas that are reviewed (e.g., exemptions, large cash transactions). References to applicable laws, regulations or other authorities are noted in parens at the end of the examination procedure.
3. As noted previously, "Know Your Customer" policies and procedures are an accepted, albeit optional, means to help prevent money laundering. The following references to "Know Your Customer" policies date from the November 1998, examination procedures revision. Further revision of these procedures, with respect to KYC, are under consideration. Meanwhile, examiners should consider explicit KYC programs to be optional. When a savings association chooses to implement a KYC program, the examiner may use the standards called for in

these procedures to help evaluate the program. In the absence of voluntary KYC programs, examiners will review the program adopted by the savings association, determine its ability to adequately identify and control the risks of exposure to money laundering activities, and evaluate the savings association's adherence to the program.

### **Off-Site Examination Planning**

Note: Section 110 of this Handbook discusses pre-examination analysis and scoping. The following discusses those items in the context of the BSA portion of an examination.

1. Review previous examination and supervisory activities to ascertain the institution's history of BSA compliance, including previous examination reports and related correspondence, and any available information from FinCEN or other outside sources. If any violations or serious deficiencies were noted, ensure in the on-site examination that the institution instituted appropriate corrective action.
2. Review the criminal referral database to determine the existence of any instances of suspicious activity or alleged illegal activity.
3. Review a list of CTRs obtained from the IRS database to determine whether the institution or any branch had a significant change in the total volume of CTR filings compared to the previous examination. The examiner may want to: (1) include a similar request in the PERK package to review similar correspondence that the institution may have received relating to incorrect or incomplete CTRs; and  
(2) verify during the on-site examination that the institution instituted appropriate corrective action.

### **Internal Compliance Programs and Procedures**

1. Verify that the institution established written policies and operating procedures required by 12 CFR 563.177.
2. Review the written compliance program to ensure that it:

- a) Provides for a system of internal controls to ensure ongoing compliance (Section 563.177©(1)).
  - b) Provides for independent testing for compliance conducted by either institution personnel or an outside party (Section 563.177©(2)).
  - c) Designates a qualified individual(s) responsible for coordinating and monitoring day-to-day compliance (Section 563.177©(3)).
  - d) Provides for training for appropriate personnel (Section 563.177©(4)).
  - e) Is approved by the institution's board of directors and noted in the minutes (Section 563.177(b)).
  - f) Includes procedural guidelines for meeting the reporting and recordkeeping requirements of the BSA regulations.
  - g) Includes procedural guidelines for the detection, prevention, and reporting of suspicious transactions related to money laundering activities.
3. Verify that the procedural guidelines include the following:
- a) The filing of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to the financial institution, which involves a transaction in currency of more than \$10,000 (CTR, IRS Form 4789) (Section 103.22(a)(1)).
  - b) The maintenance of a centralized list containing each exemption granted, with the supporting information prescribed in Section 103.22(f) and, for exemptions granted after 10/27/86, the statement and language required in Section 103.22(b)(2).
  - c) The filing of U.S. Customs Form 4790 for each shipment of currency or other monetary instrument(s) in excess of \$10,000 out of the United States or into the United States, except via common carrier, by, or to the institution (Section 103.23(a)).
  - d) The maintenance of required records for each monetary instrument purchase or sale for currency in amounts between \$3,000 and \$10,000, including the supporting information prescribed in Section 103.29(a).
  - e) The annual filing of "Report of Foreign Bank Financial Accounts" (Treasury Form 90-22) of each person, subject to the jurisdiction of the United States, who has financial interest in, or signature authority over, a bank, securities or other financial accounts in a foreign country (Section 103.24).
4. Verify that the procedural guidelines are adequately communicated to responsible personnel and that they are followed.
5. Determine whether the institution's written procedural guidelines for record retention include the retention of either the original, microfilm, copy or other reproduction of the items listed below, and whether each item is retained for at least five years:
- a) Each CTR (IRS Form 4789) (Section 103.27(a)(3)).
  - b) Documentation to support each exemption granted after October 27, 1986, and after the exemption has been discontinued (Section 103.22(d)).
  - c) Documentation to support each extension of credit over \$10,000, except when the extension is secured by an interest in real property (Section 103.33(a)).
  - d) Each advice, request, or instruction received regarding a transaction that results in the transfer of funds, currency, checks, investment securities, or other monetary instruments or credit, of more than \$10,000 to a person, account, or place outside the United States (Section 103.33(b)).
  - e) Each advice, request, or instruction given to another financial institution or other person located within or outside the United States, regarding a transaction intended to result in a transfer of funds, currency, checks, investment securities, other monetary instruments or credit,

- of more than \$10,000 to a person, account, or place outside the United States (Section 103.33©).
- f) Each payment order of \$3,000 issued in connection with wire (funds) transfer activity as an originating, intermediary or beneficiary institution (Section 103.33(e)).
  - g) A list of each individual, including the name, address, and account number, who holds a deposit account for which the institution has been unable to secure a taxpayer identification number from that person after making a reasonable effort to obtain the number (Section 103.34(a)(1)(ii)).
  - h) Each document granting signature authority over each deposit account (Section 103.34(b)(1)).
  - i) Each statement, ledger card, or other record of each deposit account showing each transaction involving the account, except those items listed in Section 103.34(b)(2-4).
  - j) Each document relating to a transaction of more than \$10,000 remitted or transferred to a person, account or place outside the United States (Section 103.34(b)(5,6)).
  - k) Each check or draft in excess of \$10,000 drawn on or issued by a foreign bank which the domestic bank has paid or presented to a nonbank drawee for payment (Section 103.34(b)(7)).
  - l) Each item relating to any transaction of more than \$10,000 received on any one occasion directly and not through a domestic financial institution, from a bank, broker, or dealer in foreign exchange outside the United States (Section 103.34(b)(8,9)).
  - m) Records prepared or received by a bank in the ordinary course of business which would be needed to reconstruct a demand deposit account and to trace a check in excess of \$100 deposited in such demand deposit account (Section 103.34(b)(10)).
  - n) A record containing the name, address, and taxpayer identification number, if available, of any person presenting a certificate of deposit for payment, as well as a description of the instrument and the date of the transaction (Section 103.34(b)(12)).
  - o) Each deposit slip or credit ticket reflecting a transaction in excess of \$100 or the equivalent record for direct deposit or other wire transfer deposit transactions. The slip or ticket shall record the amount of any currency involved (Section 103.34(b)(13)).

**Internal Controls**

1. Determine whether the institution has implemented an internal audit, management review or self-assessment program that reviews: (1) the institution's compliance program; (2) internal controls to prevent money laundering; and (3) compliance with BSA regulations. Review the adequacy of the audit scope, management review, or self-assessment program, based on the volume and types of BSA-related transactions at the institution.
2. Verify that the audit procedures:
  - a) Confirm the integrity and accuracy of the systems for the reporting of large currency transactions.
  - b) Include a review of tellers' work and Forms 4789 and 4790.
  - c) Confirm the integrity and accuracy of the institution's recordkeeping activities.
  - d) Test adherence to the in-house record retention schedule.
  - e) Include steps necessary to ascertain that the institution is maintaining the required list of exempt customers.
  - f) Test the reasonableness of the exemptions granted.
  - g) Include steps necessary to ascertain that the institution has procedures in place for maintain-

ing required information from customers purchasing monetary instruments for cash in amounts between \$3,000 and \$10,000 inclusive and that appropriate identification measures are in place.

- h) Include steps necessary to ascertain that the institution is conducting an ongoing training program.
- i) Include steps necessary to ascertain that the institution is monitoring cash shipments to and from the Federal Reserve Bank or its correspondent bank(s).

### **Anti-Money Laundering Program**

Note: Following are examination procedures that pertain specifically to anti-money laundering activities. However, other examination procedures also include anti-money laundering elements (e.g., education and training, internal controls, currency flows, etc.).

- 1. Determine whether written policies or operating procedures governing the BSA and anti-money laundering activities:
  - a) Define money laundering in its different forms (e.g., placement, layering, and integration).
  - b) Address compliance with applicable anti-money laundering laws and regulations (e.g., 12 CFR 563.177, 31 CFR 103).
  - c) Establish a “Know Your Customer” program, including account opening, identification, monitoring, and reporting procedures.
  - d) Identify potentially high risk activities, businesses, and foreign countries commonly associated with money laundering.
- 2. Verify that the anti-money laundering policies apply to all operations of the institution, including: (1) activities, including teller and currency operations, the sale of monetary instruments, wire transfers, safe deposit box; (2) departments, including trust, loan, international, discount brokerage; and (3) other operations, including correspondent and private banking.

- 3. Determine whether management has implemented a high level of internal controls to minimize the risk of money laundering. These controls should include, at a minimum:

- a) Money laundering detection procedures, including sound policies and procedures, “Know your Customer” policies, periodic account monitoring, and education and training.
- b) Identification and monitoring of non-bank financial institutions that are depositors of the institution and that engage in a high volume of cash activity (e.g., money transmitters and check cashing businesses).
- c) Periodic account activity monitoring, particularly in accounts considered high risk.
- d) Internal investigations, monitoring, and reporting of suspicious transactions.

### **Know Your Customer Policy**

Note: As discussed in the narrative section, “Know your Customer” policies or procedures are strongly encouraged as means to prevent money laundering. Appropriate policies and procedures should address the following guidelines, at a minimum:

- 1. For personal accounts:
  - a) The procurement of proper identification from the customer (e.g., driver’s license with photograph or U.S. passport or alien registration card together with a major credit card).
  - b) Consideration of a customer’s residence or place of business.
  - c) Consideration of the source of funds used to open the account.
  - d) Contact with a service bureau, if applicable, to determine whether a customer has been reported for undesirable situations (e.g., overdrawing funds, potentially conducting check kiting schemes, etc.)
- 2. For business accounts:

- a) Verification of the legal status of a business (e.g., sole proprietorship, partnership, etc.).
  - b) Verification of the name of the business with a reporting agency.
  - c) For foreign business accounts, proof that the business is registered in the country of origin (e.g., articles of incorporation).
  - d) For large commercial accounts, information relating to financial statements, the customer's principal line of business and the type of business operations performed (e.g., wholesale or retail), and a list of major suppliers and customers.
3. Determine whether the institution uses fictitious names for customers on the general ledger or other documents. If yes, verify that the institution maintains files containing the customers' real names and other identifying information, and ensure that the institution has knowledge of these customers' activities.
  4. Determine if the institution has ongoing monitoring systems in place to identify suspicious transactions (e.g., structuring, concentration accounts, transactions inconsistent with the nature of a customer's stated business, or unusual wire activities).
- e) Examples of money laundering cases and the ways in which they can be detected, resolved and reported.
  - f) The different forms that money laundering can take (e.g., deposit accounts, wire transfers, loans, etc.).
  - g) Wire (fund) transfer activity.
  - h) Overall internal policies and procedures, including "Know your Customer."
2. Review the scope and frequency of training and education to determine the importance management places on those activities.
  3. Determine, through interviews with the compliance officer and other operations personnel (e.g., tellers, platform officers, branch managers), whether personnel are sufficiently knowledgeable about the BSA and the institution's procedures to ensure compliance.
  4. Review the training program to ascertain whether it includes personnel in all departments (e.g., lending, fiduciary, and international departments, discount brokerage, private banking, correspondent and specialized foreign exchange units, and cash control centers).
  5. Conduct interviews to verify that personnel from the areas covered under the preceding procedure are knowledgeable regarding the BSA requirements, possible money laundering schemes, and the identification of suspicious or unusual activities.

### **Education and Training**

1. Review the institution's program for educating appropriate employees regarding the BSA and money laundering to determine if it includes the following:
  - a) Reporting of large currency transactions and related exemptions.
  - b) Sale of monetary instruments.
  - c) Record retention requirements.
  - d) Reporting suspicious activity or alleged criminal conduct.

### **Exemptions**

1. Obtain and review the institution's list of exempt customers and any correspondence with the Internal Revenue Service or FinCEN regarding exemptions. Verify that the list is centralized in one location.
2. Ascertain that the exemption list includes the following information required by Section 103.22(f):
  - Name of business.

- Local street address.
  - Type of business.
  - Taxpayer identification number.
  - Account number.
  - Reason for exemption.
  - Indication as to whether exemption is for deposits, withdrawals, or both.
  - Dollar limit for each exemption type (deposit or withdrawal or both).
3. Determine whether the institution conducts at least an annual review of currency transaction activity to support established limits.
  4. Determine if the institution has written documentation to support the established dollar limits.
  5. Determine if the exemptions appear commensurate with the customary conduct of the customer's business activity and frequency of large cash transactions. If the responses to the preceding three procedures are satisfactory, procedures 6 and 7 below may be omitted.
  6. Obtain customer statements of account for a sixty day period for all customers on the exemption list, and review to determine whether any daily deposit or withdrawal amounts (either individual amounts or aggregated amounts) exceed \$10,000. (The amounts on the statements of account may include cash or checks).
  7. Determine the method used by exempt customers to withdraw currency in excess of \$10,000. If checks payable to "cash" are used, review canceled checks cleared during the current statement cycle and identify those items and amounts. If counter currency withdrawal tickets or counter checks are used, review tickets or checks and identify those items and amounts. Determine whether the cash portion of the withdrawals is sufficient to qualify the customer for an exemption based upon Treasury's "regular and frequent" requirement for a withdrawal exemption. Determine whether established dollar limits are reasonable by reviewing the customer's cash withdrawal activity.

8. Determine whether the exemption list includes customers that do not immediately meet the exemption procedure's eligibility requirements and thereby require special exemptions (Section 103.22(d)). If so, determine whether written correspondence from the IRS or Treasury supports the special exemptions.
9. Determine whether the exemption list contains customers who cannot be exempted under the exemption procedures (Section 103.22(b,c)).

10. For customers on the exemption list after October 27, 1986, determine that the institution maintains a signed statement from the customer(s)

attesting to the accuracy of the information supporting the exemption(s) (Section 103.22(d)).

11. If the institution ships currency to, or receives currency from, a correspondent bank, savings association, credit union, etc., determine that the names and addresses of these institutions are included on the exemption list.
12. Determine that all accounts represented on the exemption list are of a commercial and not personal nature.
13. Determine, by discussing with appropriate personnel, whether any customers have asked to be placed on the exemption list. If so, review information relating to the account for suspicious activity.
14. Determine that the institution adheres to its established policy and regulatory requirements (Section 103.22(h)) in granting exemptions.

### **Currency Flows and Reporting of Large Cash Transactions**

1. Review a sample of cash totals shipped to and received from the Federal Reserve Bank, correspondent banks or between branch offices for a reasonable period of time (generally no less than three months) or, if available, the latest FinCEN Analysis of Federal Reserve Cash Flows, for unusual activity (e.g., material variance in totals of currency shipped or re-

- 
- ceived or large denomination currency exchanged).
2. Determine, through discussions with management, the cause of any unusual activity. Also determine if the volume of CTR filings during the period is consistent with any changes in the patterns of cash activity.
  3. Review a sample of completed CTRs, whether hard copy or from computer generated filings, to determine that (as specified in Section 103.22):
    - a) CTRs are properly completed in accordance with IRS instructions.
    - b) Transaction amounts are consistent with the type and nature of business or occupation of the customer.
    - c) CTRs are filed for large cash transactions identified by tellers' proof sheets, automated large currency transaction system, or other type of aggregation system, unless an exemption exists for the customer. If an exemption exists, determine that CTRs are filed for customers who exceed their exemption limits.
    - d) CTRs are filed within 15 calendar days after the date of the transaction (25 days if magnetically filed) (Section 103.27(a)(1)).
  4. If the institution has an automated system in place to capture individual or multiple cash transactions in excess of \$10,000 on the same business day by or on behalf of the same individual, or by account, determine whether:
    - a) the system is tested to verify that it is comprehensive regarding all points of cash entry and exit; and,
    - b) the aggregation system covers all applicable areas within the institution (e.g., discount brokerage, private banking, fiduciary, or any other departments in the institution that engage in currency transactions subject to the regulation.
  5. If the institution does not have an automated system in place, determine how the institution identifies reportable transactions.
  6. If the institution has an automated system in place to capture individual or multiple cash transactions of less than \$10,000, ascertain whether the system can detect:
    - a) Evidence of structured transactions;
    - b) "Concentration accounts" (accounts that have frequent cash deposits aggregating less than \$10,000 on any business day, and relatively few transfers of large amounts out of the accounts, by check or wire);
    - c) Customers with frequent cash transactions of less than \$10,000 who have not provided tax identification numbers; and
    - d) Customers with frequent cash transactions that have provided either a foreign address or post office box as an address or have requested that the institution hold monthly statements.
  7. Review a sample of the following reports, as available, for money laundering activities:
    - a) Suspected kiting reports. These reports identify excessive activity in accounts and should be reviewed for cash activity. The account profile of an account used for money laundering can be similar to that of an account used for check kiting in that it may have a high volume of activity, matching deposits and withdrawals, or low average balances in relation to activity.
    - b) Demand deposit activity reports. These reports cover all customer and employee accounts. They generally show daily balances and accumulated deposits and withdrawals over a 30 day period. Careful review will show accounts that have changed, either in average balance or in numbers of transactions.
    - c) Incoming and outgoing wire transfer logs. These logs can identify transfers of funds out of the country or to remote banks, transfers funded by cashier's checks or money orders in amounts under the \$10,000 CTR filing threshold, and
-

other suspicious patterns for noncustomers as well as account holders. Also review incoming and outgoing facsimile logs for payment instructions related to funds transfers.

- d) Loans listed by collateral. Review for “significant” loans collateralized by cash (certificates of deposit, bank accounts). Review situations in which collateral was received by funds transfer and the collateral is from offshore banks. Inquire about the purpose and terms of loans secured largely with cash and whether payments on those loans are often received in cash, if at all. Identify loans from which the proceeds are immediately used to purchase certificates of deposit.

#### **Sale or Purchase of Monetary Instruments Over \$3,000**

1. Determine that the institution’s records include the following information required by Section 103.29(a)(1) for purchasers who have deposit accounts with the institution:
  - a) The name of the purchaser.
  - b) Date of purchase.
  - c) The type(s) of instrument(s) purchased.
  - d) The serial number(s) of each of the instrument(s) purchased.
  - e) The dollar amount(s) of each of the instrument(s) purchased in currency.
  - f) Method of verifying identity, either at the time of purchase or when the deposit account is opened.
2. Determine that the institution’s records include the following information required by Section 103.29(a)(2) for purchasers who do not have deposit accounts with the institution:
  - a) The name and address of the purchaser.
  - b) The social security or alien identification number of the purchaser.
  - c) The date of birth of the purchaser.

- d) The date of purchase.
  - e) The type(s) of instrument(s) purchased.
  - f) The serial number(s) of each of the instrument(s) purchased.
  - g) The dollar amount(s) of each of the instrument(s) purchased.
  - h) Method of verifying identity of purchaser and specific identifying information (e.g., state of issuance and number of driver’s license).
3. Determine whether the institution’s records are retained for five years and retrievable, upon request from the Treasury, within a reasonable period of time (Section 103.29©).
  4. Determine whether the institution has a system for capturing same day, contemporaneous, or multiple sales of monetary instruments to one customer totaling \$3,000 or more, and review the adequacy of that system (Section 103.29(b)).
  5. If the institution uses manual systems to identify cash sales of monetary instruments, determine that the institution’s records are sufficiently detailed to identify the method of payment for all sales or purchases of monetary instruments.
  6. If the institution uses automated systems to identify cash sales of monetary instruments, determine that the institution’s audit or management review program tests the accuracy and validity of the identification system.

#### **Wire (Funds) Transfer**

1. Determine that an audit trail of wire transfer activities exists, and that adequate separation of duties or other compensating controls are in place to ensure proper authorization for sending and receiving transfers, and for correcting posting to accounts.
2. Verify that the institution files CTRs, when applicable, for noncustomers submitting cash for funds transfers (Section 103.22).

3. If the institution sends or receives fund transfers to/from financial institutions in other countries, especially those with strict privacy and secrecy laws, ensure that amounts, frequency and countries of origin or destination are consistent with the nature of the business or occupation of the customer.
4. Determine if the institution has procedures or other effective means to monitor accounts with frequent cash deposits and subsequent wire transfers of funds to a larger institution or out of the country.

#### **Responsibilities of Originating Institutions**

1. If the originator has an established relationship with the institution, determine, for each fund transfer origination of \$3,000 or more, whether the institution retains the following records with the payment order or in the institution's files (Section 103.33(e)(1)(i)):

(Note: A customer has an established relationship with a financial institution if the customer has a loan, deposit, or other asset account, or is a person with respect to which the institution has on file the person's name and address, as well as taxpayer ID number, or, if none, alien identification number or passport number and country of issuance, and to which the institution provides financial services relying on that information.)

- a) Name and address of the originator.
- b) Amount of the payment order.
- c) Date of the payment order.
- d) Any payment instructions.
- e) The identity of the beneficiary's bank.
- f) As many of the following items as are received with the payment order:
  - \* Name and address of the beneficiary.
  - \* Account number of the beneficiary.
  - \* Any other specific identifier of the beneficiary.

2. If the originator does not have an established relationship with the institution, determine, for each fund transfer origination of \$3,000 or more, whether the institution retains the following records:
  - a) For payment orders made in person, verification that the institution required identification and a record of the verified information.
  - b) When the institution has knowledge that the person placing the payment order is not the originator, a record of the originator's taxpayer identification number (e.g., social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.
  - c) When the payment order is not made in person, a record of the name and address of the person placing the payment order, as well as the person's taxpayer identification number (e.g., social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check or credit card transaction) for the funds transfer.
3. Determine whether the information the institution must retain for originators is retrievable by reference to the name of the originator. When the originator is an established customer of the institution and has an account used for funds transfers, determine whether the information also is retrievable by account number (Section 103.33(e)(4)).
4. For transmittals of \$3,000 or more, determine whether the institution includes in the transmittal order (Section 103.33(g)(1)):
  - a) The name and, if the payment is ordered from an account, the account number of the transmitter.
  - b) The address of the transmitter, except for transmittal orders through Fedwire until

such time as the institution that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire format.

- c) The amount of the transmittal order.
  - d) The date of the transmittal order.
  - e) The identity of the recipient's financial institution.
  - f) As many of the following items as are received with the transmittal order:
    - \* The name and address of the recipient
    - \* The account number of the recipient
    - \* Any other specific identifier of the recipient; and either the name and address or numeric identifier of the transmitter's financial institution.
5. Determine whether the institution is complying with the FFIEC's December 23, 1992 policy statement, which recommends that the text of every payment order include the name, address, and account number of the originator and beneficiary.

#### **Responsibilities of Intermediary Institutions**

1. For transmittals of funds of \$3,000 or more, determine whether the institution includes in the transmittal order to the next receiving financial institution the following, if received from the sender (Section 103.33(g)(2)):
  - a) The name and account number of the transmitter.
  - b) The address of the transmitter (except for transmittal orders through Fedwire until such time as the institution that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire format).
  - c) The amount of the transmittal order.
  - d) The date of the transmittal order.

- e) The identity of the recipient's financial institution.
- f) As many of the following items as are received with the transmittal order:
  - \* The name and address of the recipient.
  - \* The account number of the recipient
  - \* Any other specific identifier of the recipient; and either the name and address or numeric identifier of the transmitter's financial institution.

#### **Responsibilities of Beneficiary Institutions**

1. For payment orders of \$3,000 or more received for a beneficiary that is not an established customer of the institution (Section 103.33(e)(3)):
  - a) If proceeds are delivered in person to the beneficiary or its representative or agent, determine that the institution verified the identity of the person receiving the proceeds and obtained and retained a record of that information.
  - b) If the institution has knowledge that the person receiving the proceeds is not the beneficiary, determine that the institution obtained and retained a record of the beneficiary's name and address, as well as the beneficiary's identification.
  - c) If the proceeds are delivered other than in person, determine that the institution retained a copy of the check or other instrument used to effect the payment, or the information contained thereon, as well as the name and address of the person to which it was sent.
2. Determine whether the information that the institution must retain for beneficiaries is retrievable by reference to the name of the beneficiary, and, if the beneficiary is an established customer of the institution and has an account used for fund transfers, whether the information also is retrievable by account number (Section 103.33(e)(4)).

**Payable Through Accounts**

1. Review the contracts/agreements with foreign banks, if applicable. Determine whether they:
  - a) Address procedures for opening sub-accounts.
  - b) Provide the U.S. institution with the ability to appropriately identify sub-account holders.
  - c) Prohibit cash transactions by sub-account holders within U.S. borders.
  - d) Require the foreign bank to monitor sub-account activities to detect, report, and investigate suspicious or unusual transactions and report findings to the U.S. institution.
  - e) Clearly state the liability of both the U.S. institution and the foreign bank to which the payable through accounts service is being offered.
2. Review the institution's system of internal controls for opening and monitoring payable through accounts and determine whether it provides for:
  - a) Procedures for opening accounts.
  - b) Operational procedures.
  - c) Staff responsibilities.
  - d) Training.
  - e) Audit.
  - f) Identifying and reporting of unusual or suspicious transactions.
3. Determine whether the institution's "Know Your Customer" policy is applied to payable through accounts.
4. Determine whether the institution prohibits foreign banks from opening sub-accounts (second tier) for other foreign banks, casas de cambio's, finance companies or other financial intermediaries. If they are permitted, determine the procedures used by the institution to understand the identity of the second tier sub-account holders and the nature of the business transactions.
5. Determine whether the institution periodically reviews the listing of account and sub-account holders to ensure that no accounts have been opened for individuals or businesses located in countries that are prohibited from doing business in the U.S. as determined by the Treasury's Office of Foreign Assets Control (see "Economic Sanctions," Handbook section 415).
6. Determine if the institution monitors account activity for unusual or suspicious transactions, and whether foreign banks that maintain the payable through relationship review and explain suspicious transactions
7. Determine whether the institution prohibits cash transactions by sub-account holders. If not, determine whether the institution properly completes CTRs for large cash transactions.
8. If possible, determine whether the home country supervisor of the foreign bank requires banks to identify and monitor the transactions of their customers consistent with U.S. requirements.
9. Determine whether the institution obtains adequate information about the ultimate users of the payable through accounts.
10. Determine whether the institution can ensure that its payable through accounts are not being used for money laundering or other illicit purposes, and if it cannot, determine whether the institution has taken steps to terminate account relationships as expeditiously as possible.
11. Determine whether the institution maintains adequate information (e.g., financial statements, licensing confirmation, etc.) regarding the foreign bank.

12. Evaluate the method (e.g., audit or other review) used by the institution to ascertain:
- a) The procedures of the foreign bank for opening accounts, to determine if they are consistent with U.S. requirements.
  - b) The foreign bank's monitoring of sub-account activities to detect and report suspicious or unusual transactions.